

REMARKS

In the Office Action¹, the Examiner rejected claims 1-5, 13-15, 20-24, 32-36, 44-46, and 51-55 under 35 U.S.C. § 103(a) as unpatentable over JP 10-65662 to Ishiguro et al. ("*Ishiguro*") in view of U.S. Patent No. 6,314,409 to Schneck et al. ("*Schneck*"), U.S. Patent No. 6,374,036 to Ryan et al. ("*Ryan*"), and "Applied Cryptography" by Schnier ("*Schnier*").

Applicants respectfully traverse the rejection of claims 1-5, 13-15, 20-24, 32-36, 44-46, and 51-55 under 35 U.S.C. § 103(a). Independent claim 1, for example, recites an information-signal playback system comprising an information-signal reading apparatus and an information-signal processing apparatus, the information-signal reading apparatus comprising, among other things, an output means for supplying, to the information-signal processing apparatus, "said information on said copyright protection as encrypted by said encryption means, and said same information on said copyright protection in an unencrypted form." The cited references fail to teach or suggest the claimed output means.

The Examiner concedes that *Ishiguro* fails to disclose the claimed output means (Office Action at p. 3). However, the Examiner alleges, "*Schneck* discloses the output means for supplying the information on copyright protection encrypted by the encryption

¹ The Office Action contains a number of statements reflecting characterizations of the related art and the claims. Regardless of whether any such statement is identified herein, Applicants decline to automatically subscribe to any statement or characterization in the Office Action.

means and the unencrypted information on copyright protection" (Office Action at p. 3). Even assuming the Examiner's assertion is correct, the claimed output means supplies the "same information on said copyright protection" both encrypted and in an unencrypted form." In contrast, *Schneck* discloses, "packaged data 108 may include an encrypted version of the access rules 116, or these rules may be provided to the user separately. The logical data structure for the packaged data 108 is shown in FIG. 2 and includes an encrypted body part 120, an unencrypted body part 122, [and] encrypted rules" (*Schneck* col. 10, lines 47-53). Even assuming the packaged data in *Schneck* correspond to the claimed "information on said copyright protection," *Schneck* discloses only distinct encrypted and unencrypted body parts, not the same body part provided in both an unencrypted and encrypted state. *Schneck*, therefore, fails to teach or suggest the claimed output means for supplying, to the information-signal processing apparatus, "said information on said copyright protection as encrypted by said encryption means, and said same information on said copyright protection in an unencrypted form."

Ryan fails to cure the deficiencies of *Ishiguro* and *Schneck*. *Ryan* discloses, "a watermark ... is conventionally embedded in a video image. A subset of the watermark bits carries a digital attribute (a number) which is a numeric characteristic of the video signal, for instance an average amplitude of the video signal over one video field or frame (*Ryan* col. 3, lines 1-6). *Ryan* continues, "[t]he compliant digital video recorder ... examines the watermark, verifies it, ... and extracts the associated attribute value from the watermark. The compliant recorder also ... measures the attribute of that particular field, and compares the measured attribute to the extracted attribute value" (*Ryan* col. 3,

lines 26-36). Thus, the attribute value in *Ryan* cannot correspond to the claimed “information on said copyright protection,” because *Ryan* discloses pre-storing an attribute value such as the average amplitude of the signal in a frame, and subsequently measuring the attribute value. First, storing the attribute value in a watermark is not the same as storing “information on said copyright protection as encrypted by said encryption means.” Moreover, *Ryan* does not disclose storing the attribute value in another form in the video image, but rather the “compliant recorder” measures or calculates the attribute value from the video image itself. Thus, *Ryan* does not teach or suggest the claimed output means for supplying, to the information-signal processing apparatus, “said information on said copyright protection as encrypted by said encryption means, and said same information on said copyright protection in an unencrypted form.”

Schnier fails to cure the deficiencies of *Ishiguro*, *Schneck*, and *Ryan*. *Schnier* discloses a “one-way hash function .. that takes a variable-length input (called a pre-image) and converts it to a fixed-length (generally smaller) output string (called a hash value)” (*Schnier* p. 30). First, the hash function disclosed by *Schnier* does not correspond to the claimed “encryption,” as *Schnier* discloses “[t]he hash function is public; there’s no secrecy to the process” (*Schnier* p. 30). Moreover, even assuming the hash function does correspond the claimed “encryption,” *Schnier* makes no mention of providing both the hash value and the pre-image through an output means. *Schnier* therefore fails to teach or suggest the claimed output means for supplying, to the information-signal processing apparatus, “said information on said copyright protection

as encrypted by said encryption means, and said same information on said copyright protection in an unencrypted form.”

Further, Applicants disagree with the Examiner’s assertion that *Schnier* teaches the claimed “comparing means for comparing the decrypted information on said copyright protection with the unencrypted information on said copyright protection to judge if an attempt to alter the information on said copyright protection has been performed” (Office Action at p. 4). *Schnier* discloses that hash functions are “a way of fingerprinting files. If you want to verify that someone has a particular file (that you also have), but you don’t want him to send it to you, then ask him for the hash value. If he sends you the correct has value, then it is almost certain that he has the file” (*Schnier* p. 31). *Schnier* thus teaches comparing the two hash values to verify the authenticity of a file, not comparing “decrypted information ... with unencrypted information.” Indeed, because *Schnier* discloses a “one-way hash function” that is “many to one,” such a hash value cannot be “decrypted” at all. Therefore, *Schnier* fails to teach the claimed comparing means. The remaining references also fail to disclose the claimed comparing means.

Although of different scope, independent claims 13, 20, 32, 44 and 51 recite features similar to those of claim 1. Claims 2-5 depend from claim 1, claims 14 and 15 depend from claim 13, claims 21-24 depend from claim 20, claims 33-36 depend from claim 32, claims 45 and 46 depend from claim 44, and claims 52-55 depend from claim 51. As already discussed, the cited references fail to teach or suggest the claimed output means and comparing means.

The dependent claims may further recite additional features not taught by the cited references. For example, dependent claim 2 recites the information-signal reading apparatus of claim 1, "wherein said information on copyright protection is media-type information indicating the type of said recording medium," and, as discussed, claim 1 recites supplying, to the information-signal processing apparatus, "said information on said copyright protection as encrypted by said encryption means, and said same information on said copyright protection in an unencrypted form" and "comparing the decrypted information on said copyright protection with the unencrypted information on said copyright protection to judge if an attempt to alter the information on said copyright protection has been performed." The cited references fail to teach or suggest this subject matter of claim 2.

The Examiner cites to portions of *Schneck* and *Ryan* that allegedly disclose "media-type information indicating the type of the recording medium" (Office Action at p. 4). However, neither of these references discloses supplying both encrypted and unencrypted information about the type of recording medium, or comparing decrypted information about the type of recording medium with unencrypted information about the type of recording medium. Instead, the cited portions of *Schneck* merely disclose, "in a video cassette recorder ... a single control program may be running at all times ... all access to controlled data is initiated by the control program" (*Schneck* col. 18, lines 11-16). The controlled data does not correspond to the claimed "media-type information indicating the type of said recording medium," and even if it did, *Schneck* does not disclose supplying the controlled data in both encrypted and unencrypted form, or

comparing decrypted controlled data with unencrypted controlled data. *Schneck* therefore fails to teach or suggest the claimed “wherein said information on copyright protection is media-type information indicating the type of said recording medium.”

Ryan also fails to disclose this subject matter of claim 2. The cited portions of *Ryan* disclose, “[t]here is a need for a copy-once method in the digital video recording field that offers improved economics and security over the existing art. There is also a need for a copy-once method that requires only one watermark and therefore only one watermark detector per compliant recorder (or player) apparatus (*Ryan* col. 2, lines 30-35). The watermark in *Ryan* does not correspond to the claimed “media-type information indicating the type of said recording medium,” and even if it did, *Ryan* does not disclose supplying the watermark in both encrypted and unencrypted form, or comparing a decrypted watermark with an unencrypted watermark. *Ryan* therefore fails to teach or suggest the claimed “wherein said information on copyright protection is media-type information indicating the type of said recording medium.” The remaining references also fail to disclose this subject matter of claim 2.

Because the cited references fail to teach or suggest each and every claim element recited by claims 1-5, 13-15, 20-24, 32-36, 44-46, and 51-55, no prima facie case of obviousness has been established with respect to these claims. Applicants therefore request the Examiner to withdraw the rejection of these claims under 35 U.S.C. § 103(a).

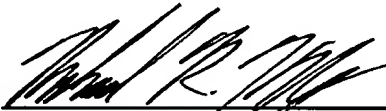
Please grant any extensions of time required to enter this response and charge any additional required fees to our deposit account 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: September 29, 2006

By:



Michael R. Kelly
Reg. No. 33,921